E-GOVERNANCE, IDENTITY, AND PRIVACY

Contents

Introduction

This chapter will look at different legislations, projects, and policies pertaining to e-governance and identity that India has put in place, and examine both the strengths and the weaknesses of these, through the lense of privacy.

Identity

In India, currently there are at least eighteen documents that are recognized as acceptable proofs of identity.[1] These range from the passport, to the ration card, to the voting card. Each of these identities serves a specific function, and none act as one comprehensive national identifier. Government issued identification is essential to the effective functioning of a State, and to the mobility of individuals in the formal structures of a country. Governments use identification to assess populations for the delivery of services, and to monitor populations within its borders. Though on one hand identification provides governments with the ability to assess population, the expansive nature of identification technologies provides governments with the ability to gather, track, retain, combine, and share personal information with ease. Thus, in recent years there has been an increase in privacy concerns surrounding identification schemes, as citizens worry that governments are reaching too deeply into their personal lives, and using identification for invasive purposes. Though technology is most readily pointed to the root cause of privacy concerns in identity schemes, privacy violations also arise from poorly crafted legislation and project design. When identity legislation is created without privacy in mind, it leads to schemes that allow for unwarranted access by authorities to personally identifying information, permits the over collection of data, and permits personal information to be used outside of the scope of identification without redressal mechanisms in place. Other privacy concerns related to identity include identity theft, impersonation, fraud, and inaccurate or incomplete information in the database.

E-Governance

Central and State Governments in India are increasingly transforming infrastructure and public services so that they are digitized and delivered via the internet and other electronic forms. For example, the State of Kerala is currently in the process of becoming a 'digital state' and moving all services from banking, citizen state communications, and everyday transactions to a digital platform. National projects range from shifting corporate transactions to e-format in order to reduce corporate fraud, to establishing one integrated database for governmental information from various departments. Though the shift to the digital allows governments to be more transparent and efficient while allowing citizens and residents to register for government services, obtain and file government forms, apply for employment, it also allows for further expanded government collection and collation of personally identifiable data. With the increasing use of technology in government-to-citizen interactions it is important to ensure that when e-government projects are implemented, they adopt integrated schemes to maintain adequate privacy safeguards prior to collecting and using data. The Indian government’s growing practice in collecting, retaining, and managing personal data without adequate privacy protection in place, pose a wide range of privacy concerns such as data mining, profiling, function creep, and inappropriate use of data.

Legislation

The Passport Act 1967: (Rules 1980)

The Indian passport is a government issued ID document that recognizes an individual as an Indian citizen, and allows an individual to pass in and out of India. The passport document is supported by the Passport Act.[2] The Act establishes the Passport Authority, a body empowered by the Central Government to issue passports or travel documents.[3] Individuals are held criminally liable for contravention of the Act. Critical information under the Act includes personally identifying information that is shared by individuals for the obtaining of a passport. Specific provisions relevant to privacy include:

- *Wrongful Possession:* The Passport Authority may impound or revoke passports or travel documents if they are satisfied that the holder of the document is not the rightful owner.[4] This touches on both the privacy violation of impersonation and identity theft. This provision protects privacy by ensuring that individuals cannot use another's identity.
- *Fraud*: The Passport Authority may impound or revoke passports or travel documents if it is found that the person obtained the passport on the basis of false information.[5] This provision protects privacy as it prevents against the issuance and use of fake documents.
- *Notification to individual*: If the Authority chooses to revoke or impound a passport the reasons must be recorded in writing, and a copy of the demand must be furnished to the passport holder, unless the authority finds it to be not in the interest of the sovereignty and integrity of India, the security of India, friendly relations with any foreign country or in the interests of the general public to furnish a copy.[6] This provision protects privacy as it ensures that individuals are informed as to the status of their identification document and the reasons thereof.
- *Appeal*: An individual aggrieved by an order from the Passport Authority may submit an appeal to the appellate authority against the order of the Authority. No appeal is allowed to be made against an order from the Central Government.[7] This provision protects privacy as it protects individuals from unjust or inaccurate orders relating to their identity.
- *Offenses and Penalties*: Among other offenses, individuals who knowingly furnish false information, fail to produce for inspection his/her passport or travel documents when required to by the prescribed authority, knowingly uses a passport issued to another person, or knowingly allows another person to use his/her passport is punishable with imprisonment for 1-5 years and a fine which may extend to Rs. 5,000.[8] Individuals who possess a forged passport or travel document face imprisonment of 1-5 years and a fine which may extend to 50,000 rupees.[9] Both these penalties protect privacy. The severity of the penalty imposed for use of a forged passport in comparison to simply using another person's passport creates a higher standard for the use of fraudulent identities.
- *Power to arrest without warrant*: Any customs officer may arrest without warrant any person who is reasonably suspected of committing an offence under the Act.[10] Though it is important that customs officers have the ability to detain individuals who are in contravention of the Act, to protect against unreasonable arrest, the Act should require that the officer obtain a warrant for the arrest within a specified time period from the arrest.

- *Search and Seizure:* Any customs officer empowered by the Central Government, empowered by a general or a special order by the Central Government may search and seize any passport or travel document where there is reasonable suspicion that he/she has committed an offence under the Act. The standards for search and seizure found in the Cr.Pc. apply to this Act.[11] Though this is a broad standard which could impact privacy, the fact that individuals are able to make appeals under the Act, creates a safeguard for the individual if this provision is abused.

The Representation of People Act 1950: (Rules 1960, 1961, 2011)

Elections in India are held according to constitutional provisions, and supplemented by laws made by Parliament. The Representation of the People Act, 1950[12] lays out standards and procedures for the preparation and revision of electoral rolls, the carrying out of elections, and the resolution of post election disputes.[13] Penalties under the Act are both criminal and civil. The Election Commission of India (ECI) is the permanent constitutional body responsible for overseeing elections in India and is given powers analogous to a civil court.[14] One of the functions of the ECI is to prepare electoral rolls of registered voters in all assembly constituencies in India, and more recently, to issue photo identity cards (EPIC) to all voters. Aspects of the Act that relate to privacy include:

- *Access to information:* For the purpose of preparing the electoral rolls, a registration officer may access copies of the Register of Births and Deaths and the admission register of any educational institution in any area.[15] The access to information that is permitted in this provision does not directly impact privacy, but the provision could be strengthened by clearly defining what information is allowed to be accessed and how that information will be used.
- *Collection of information:* Preparation of the electoral rolls is through house to house collection and verification of information. Registration is based on locale, and an individual is only permitted to be registered in one place. Collection of information is clearly necessary for the preparation of the electoral rolls. This provision could be strengthened by putting in place safeguards that would prevent against the possibility of over collection of non-relevant information.
- *Proactive disclosure:* The complete electoral rolls – containing details such as full name, relatives, age, sex and EPIC number are required by law to be available for inspection at the office of the registration officer, and copies of the rolls must be supplied to every political party.[16] This provision could potentially invade privacy because of the granularity of information that is displayed.
- *Individual Access:* All citizens may obtain copies of extracts of the rolls pertaining to themselves upon payment of a fee.[17] In addition, it has become common practice for state election commission websites to provide online access to complete lists of electoral rolls that they maintain.[18] This provision protects privacy by allowing individuals to access personal information that is held about them by organizations and the government.
- *Confidentiality*: Individuals who perform duties that are in connection with the counting of votes at an election must maintain and assist in maintaining the confidentiality of the voting. Contravention of this provision is penalized with imprisonment of up to three months and or a fine.[19] This provision protects privacy as it categorizes information relating to a vote as sensitive information that must be kept confidential.
- *Penalty for influence*: Any officer connection to an election or member of the police

who tries to persuade, dissuade, or influence any individual from voting will be imprisoned for up to six months.[20] This provision protects privacy as it maintains that individuals have the privacy to make the decision to vote, and for whom without interference.

- *Penalty for tampering:* Among other penalties, the Act punishes with imprisonment any individual who destroys, takes, opens, or interferes with ay ballot box or ballot papers.[21] This provision protects privacy as it acts as a safeguard to protect the confidentiality and integrity of votes.
- *Penalty for false information:* Any candidate who fails to furnish required information under the Act, conceals information, or provides false information is punishable with imprisonment for a term which could extend to six months.[22] This provision protects privacy as it ensures transparency in the election process and ensures that individuals are accurately informed about who they are voting for.

The Indian Penal Code 1860

- *Impersonation:* Whoever falsely personates another, and in such assumed character makes any admission or statement, or confesses judgment, or causes any process to be issued or becomes bail or security, or does any other act in any suit or criminal prosecution, shall be punished with imprisonment of either description for a term which may extend to three years or with fine, or with both.[23]

Information Technology Act 2000

- *Penalty for Identity Theft& Fraud:* Any person who fraudulently or dishonestly makes use of an electronic signature, password, or unique identification feature, or uses a communication device or computer resource to impersonate another individual is held criminally and civilly liable. Any person who uses a communication device or computer resource to cheat by impersonation is also held criminally and civilly liable.[24]

The Indian Income Tax 1961

In India taxes are regulated and monitored through an individual's ten digit PAN number. The number is issued by the Tax Authority of India, in order to facilitate the interlinking of all financial transactions related to an individual.[25] The Income Tax Authority is vested with judicial powers analogous to a civil court.[26] Specified officers under the Act are vested with powers analogous to a court under the Code of Criminal Procedure.[27] The Act establishes an Appellate Tribunal for purposes of hearing complaints and cases filed under the Act. Individuals in contravention with the Act are held liable with civil and criminal penalties. According to the Tax Department, "PAN enables the department to link all transactions of the "person" with the department. These transactions include tax payments, TDS/TCS credits, returns of income/wealth/gift/FBT, specified transactions, correspondence, and so on. Thus, the PAN card acts as an identifier of a "person" to the tax department".[28.] Provisions in the Act that pertain to privacy include:

- *Pro-active disclosure*: Every person in possession of a PAN number must quote his number on all returns or correspondence with the income tax authority, in all challans for the payment of any sum due, to any person responsible for deducting tax from his/her income, if he/she is a buyer or licensee, and in all documents pertaining to transactions which the Board has determined and indicated.[29] This provision pertains to privacy as it determines the instances in which an individual must identify themselves and quote their PAN number.

- *Collection:* The Central Government may collect any information which is useful or relevant for the purposes of the Act.[30] Similarly, the income tax authority may, for purposes of collection information that might be useful or relevant for the purposes of the Act enter into any building or place within the limits or assigned to the authority.[31] This provision pertains to privacy has it lays out the types of information that can be collected by the Central Government. Currently, the provision is broad and potentially invasive of privacy as it allows the government to collect any information that is useful.
- *Updation of information*: Individuals must inform the Assessing Officer of any change in address, name, or nature of business on which his/her original PAN number was based.[32] This provision protects privacy by requiring that individual tax information is up to date.
- *Safeguards:* Under the Act designated officers have the power to impound and retain custody of documents and account books only if the reasons are recorded in writing. Any book or document that is impounded cannot be retained for more than fifteen days without obtaining approval.[33] These safeguards protect privacy by ensuring that information is not unreasonably obtained or retained for longer than necessary.
- *Disclosure in public interest:* Any specified authority can disclose any information received if it is determined to be in the public interest.[34] The Central Government may publish the names of any assesses and any other particulars relating to any proceedings or prosecutions if it finds it necessary or in the public interest to do so.[35] This provision impacts privacy by maintaining 'public interest' as an exception to the confidentiality of information.

The Census Act, 1948: (Rules 1990)

Census is the counting of citizens of India, and is an instituted method of gathering information about Indian society. Every person within the boundaries of India is enumerated regardless of sex, caste, religion, nationality and age, including the homeless and slum dwellers. The legitimacy of the census data and the fact that it is statutory exercise with constitutional backing that impacts the political representation of many indigenous and religious groups makes the protection and confidentiality of census data important and relevant to the privacy of an individual. The information is collected manually through house to house enumeration, and then compiled electronically. Privacy risks associated with the electronic compilation of personal information collected for the census include the practice of linking individuals' identities to anonymous census records, using census information for marketing purposes, and the possibility of political abuse. By appointment from the Central Government, the Act establishes a Census Commissioner, District & Deputy Collectors, Charger Officers, Supervisors, and Enumerators. The Act puts in place strong safeguards over data collected for the census by creating criminal penalties for contravention of the Act. Aspects of the Act which relate to privacy include:

- *Proactive Discovery*: The Central Government, for the purposes of using a property which may be needed to carry out the census, may require any individual to furnish information needed to any specified authority.[36] This provision creates an exception to privacy as it lays out circumstances for when individuals must disclose information to officials.

- *Inspection*: Any person authorized by the Central Government may enter into a premise and inspect the premise to determine if it is needed for the carrying out of the census.[37] This provision creates an exception to an individual's right to privacy as it lays out circumstances of when the Government may enter and inspect a premise.
- *Confidentiality:* Inspection of any book, register, or record that is made by a census officer is prohibited. Furthermore, except as laid out in the Indian Evidence Act, entries into of a census book, register, etc shall not be used as evidence in a civil proceeding or criminal proceeding, except for a prosecution under the Act or any other law.[38] This provision protects the privacy and confidentiality of information collected by census officers.
- *Public disclosure*: The Census Commissioner is responsible for determining data can be released to the public.[39] This provision protects privacy by establishing that only the Commissioner can have the power to determine when potentially confidential census data can be released to the public.
- *Unlawful disclosure*: Any Census Officer who knowingly discloses any information which he has received through the census is held liable to punishment of a fine of Rs. 1000 and imprisonment which may extend up to three years.[40] This provision protects privacy by creating an offense for the disclosure of census data.
- *Unlawful manipulation:* Any Census Officer who removes, secretes, damages or destroys a census document is held liable to punishment of a fine of Rs. 1000 and imprisonment which may extend up to three years.[41] Additionally, any person who removes, obliterates, alters, or damages any letters, marks or numbers that affixed for the purpose of the census are held liable to punishment of a fine of Rs. 1000.[42] This provision protects privacy by ensuring the integrity of census data.
- *Accuracy:* The District/Additional District or Sub-Divisional Census Officer, among other duties, is in charge of preparing and maintaining up to date and accurate lists of villages and towns[43] The Charge Officer will be responsible for ensuring full coverage, accuracy, and adherence to time lines in taking the census.[44] The Enumerator is responsible for updating records and updating house numbering.[45] Any Census Officer who knowingly makes any false return is punishable with a fine and imprisonment.[46] This provision protects privacy by ensuring the accuracy of census data.
- *Collection:* The Supervisor is responsible for collecting the filled in forms from each enumerator and forwarding these documents to the Charge Officer within two days of completing the census operations.[47] The Enumerator will also be responsible for handing over all documents under his/her possession to the Supervisor.[48] This provision protects privacy by establishing a procedure that is to be followed for the collection of census data.
- *Storage*: After completion of the census, the canvassed census schedules will be kept in the office of the Director Census Operations or any other place that the Director of Census Operations designates.[49] After processing, canvasses schedules will be preserved at the office of the Director of Census Operations or at such other place where he may direct.[50] This provision protects privacy by establishing a protocol for the storage of census data.
- *Aggregation:* The Census Commissioner or Director of Census Operations may use and publish extracts from information collected through the census for statistical purposes. [51]
- *Data Retention*: Census schedules and other connected papers will be retained until the year before the next census. At that point the relevant documents will be disposed

of.[52] This provision protects privacy by establishing a data retention regime, thus ensuring that census data is not retained for longer than is necessary.

- *Missing Safeguards*: Though the census provides strong safeguards that protect the privacy of collecting data, the Act and Rules are missing regulations and procedures for how census data will be processed, stored, retained, and destroyed electronically.

The Citizenship Act, 1955: (Citizenship (Registration of Citizens and Issue of National Identity Cards) Rules, 2003 and the Citizenship Rules, 2009)

The Indian Citizenship Act[53] establishes the legal basis for citizenship to India. The issuing of National Identity Cards is legalized under the Citizenship Act. To implement the issuance of identity cards the Act creates the National Registration Authority, which is filled by the Registrar General (the Registration of Births and Deaths Act, 1969).[54] The National Register of Indian Citizens is a collated database containing information of citizens residing in and outside of India. Information from five smaller databases is inputted into the database. The five data bases include: the sub-district Registrar of Indian Citizens, State Registrar of Indian Citizens, the population registrar, Local Registrar of Citizen Registration, and the District Registrar of Indian Citizens. The Act requires that each register contain an individual's name, father's name, mother's name, sex, date of birth, place of birth, residential address, marital status, visible identification mark, date of registration of citizen, serial number of registration, and national identity number.[55] The Citizenship Act and Rules establish a Tribunal for hearing complaints and answering questions asked by individuals.[56] The Act prescribes criminal and civil penalties for contravention of its provisions. Aspects of the Act which pertain to privacy include:

- *Identity*: The Central Government will register every citizen of India and subsequently issue national identity cards. In doing so the government may maintain a National Register.[57] This provision does not directly protect or violate privacy, but allows for the issuance of a card that contains information requiring privacy protection.
- *Collection:* For the purpose of an identity card, the relevant data is meant to be collected through house to house enumeration. Further procedures for preparing the National Register will be determined by the Register General.[58] This provision establishes how information will be collected, but does not fully protect privacy as it does not ensure against the over collection of information by officials conducting the house to house enumeration.
- *Reactive Disclosure:* Every Citizen is held legally responsible for registering himself/herself with the Local Registrar of Citizen Registration and for providing accurate information.[59] It is also the duty of every individual to inform the District Registrar within a period of thirty days if they have ceased to be citizens of the country.[60] This provision impacts privacy by placing the burden of registration and accuracy on the individual.
- *Proactive Discovery*: All persons must furnish to the appropriate authority information within his/her knowledge pertaining to the status of an individual's citizenship. The District Registrar, Sub-district or Taluk Registrar or the Local Registrar of Citizen Registration is given the authority under the Act to require that individuals furnish this information.[61] This provision establishes circumstances for when individuals are required to disclose sensitive information to officials. Though the Act establishes who has the authority to require disclosure from individuals, it does not require any further safeguards such as an order or a request in writing. This lack of safeguard could

potentially violate the privacy of individuals.

- *Transparency:* As a form of verification, the draft of the Local Register of Indian Citizens will be published with the invitation for objections or for inclusions of any name or particular information[62]. If there is an objection against a particular entry or a need for the inclusion of an entry, this may be submitted to the Local Registrar for correction within 30 days of the publication.[63] Though this provision works to bring transparency to the process of registration, it has the potential to violate the privacy of an individual as it takes away the right of anonymity surrounding an individual's citizen status.
- *Inspection:* Any Registrar or Officer who has been authorized by the Registrar General of Citizen Registration may examine any record, and issue directions regarding inclusion or exclusion of particulars from the population register or local register of Indian Citizens.[64] This provision protects privacy by requiring that officials obtain authorization from a higher authority before accessing sensitive information.
- *Breach Notification:* There are three instances when the government is required to inform an individual that their records have been accessed, or give justification for the Governments actions. 1. If the government intends to withdraw Citizenship from an individual they are required, before making the order, to give notice in writing and give the individual the right to make an application for his case.[65] 2. With regards to information stored in the National Registrar, if an individual's record is examined, the individual should be informed of the reasons for such examination and the results. 3. If an individual's particulars are deleted from the National Registrar because of death, the relatives of the individual will be informed.[66] This provision protects privacy by ensuring that individuals are notified when their data is examined, altered, or deleted.
- *Fraud:* If registration or certificate was obtained by fraud, false representation, or concealment of any fact – the Central Government will withdraw citizenship.[67] Any person who knowingly makes a false representation for procurement of anything under the Act will be held criminally liable.[68] Any person who knowingly makes a false representation of any material will be imprisoned for up to five years and a fine which can extend to Rs. 50,000.[69]This provision protects privacy by penalizing the use of fraudulent information.
- *No notification required:* If the Central Government refuses a normal application for citizenship, the officer is not required to give reason for the denial.[70] This provision does not protect privacy as it does not ensure that an individual is fully informed as to the reasons that they have been denied citizenship.
- *Verification and Identity:* The Local Registrar is required to verify and scrutinize the collected particulars of every family. If the Local registrar finds any information provided doubtful, it will be noted, and the individual will be informed.[71] This provision protects privacy as it verifies the accuracy of the information collected.
- *Appeal:* If an individual's particulars are found doubtful, they will be given the right to be heard by the Sub-district Registrar.[72] Additionally, any person aggrieved by the order of the sub-district or Taluk Registrar may make an appeal within thirty days of a specific order.[73] Any person who is harmed by an order made under the Act may, within 30 days of the order, may apply for a review of the order by the Central Government. These provisions protect the privacy of individuals by giving them the right to appeal and seek revision for any decision made with concern to personal information about their citizenship.
- *Deletion:* Individual details will be deleted from the National Register by an order from the Registrar General if an individual ceases to be a citizen, in the event of a death, if

an individual's Citizenship is revoked, or the particulars provided are incorrect.[74] This provision protects privacy by creating clear circumstances for when information can be deleted.

- *Maintenance:* The Registrar General will be responsible for maintaining the National Register of Indian Citizens in electronic or some other form and up to date on the basis of extracts from various Registers specified under the Births and Deaths Act.[75] This provision protects privacy by creating an authority who is responsible for maintaining information that is collected and stored up to date.
- *Modification:* The sub-district or Taluk Registrar may, on application by the concerned person and after due verification, modify an entry in respect to the particulars of an Indian Citizen including: change of name, change of parent's name, change of address, change of marital status, change of sex.[76] This provision protects privacy by clearly designating an official who is responsible for making changes to stored information.

The Registration of Births and Deaths Act, 1969

This Act[77] provides for the regulation of registration of births and deaths in India. The database of births and deaths is used by both for the census and for the National Indian Database. Privacy is relevant to this Act when understanding how records are registered, maintained, and accessed. The Act creates the Registrar of India as the overseeing Authority in charge of implementing the provisions of the Act. Authorities under the Registrar General include the Chief General, the District Registrar, and Registrars.[78] Civil penalties are prescribed by the Registrar General for offenses committed under the Act.[79]

- *Access:* Any individual may search any entry in a register of births and deaths or obtain an extract.[80] Privacy is protected as no extract relating to any death may give detail of the particulars regarding the cause of the death entered into the register.
- *Copy of records:* The Registrar will give to the person registering a birth or death a copy of the extract free of charge.[81] This provision protects privacy as it allows individuals to freely access information.
- *Correction, accuracy, and cancellation:* Only the registrar, if satisfied that an entry in the register is incorrect or fraudulent, may correct, alter, or cancel entry.[82] This provision protects privacy by designating an official who is authorized to change or delete entries in the register.
- *Collection:* The Chief Registrar is responsible for compiling and standardizing the prescribed forms for registration.[83] This provision protects privacy by designating an official responsible for creating a standardized procedure for the collection of information. To further protect privacy the procedure for compilation and collection should be laid out in Rules under the Act.
- *Inspection:* Registration offices and registers are to be inspected and examined by the District Registrar.[84] This provision protects privacy by putting in place an accountability mechanism.
- *Aggregation:* The Chief Register will be responsible for compiling and publishing the collected information in a statistical report.[85] This provision protects privacy by designating an official who is responsible for the aggregation of data. The Act could further protect privacy by establishing standards such as anonymization that must be followed when aggregating data.
- *Proactive Discovery:* The Registrar may orally or in writing require any person to

furnish information that is in connection with a birth or death. The individual is required to comply with such a request. Failure to do so results in a fine.[86] This provision impacts privacy by creating a standard for when information must be disclosed to officials.

- *Maintenance of Records:* The State and Central Government is enabled to:
  - make rules concerning the manner in which records of births and deaths are to be given in,
  - grant the search of the birth and death register,
  - allow for extracts from the registers to be copied
  - determine the form in which the returns and statistical report will be published,
  - determine the custody, production, and transfer of registers and other records,
  - provide for the correction of errors and the cancellation of entries of births and deaths.[87] This provision establishes that the Central Government has the authority to make rules that will impact the protection of the data.

Information Technology Act 2000: (Electronic Service Delivery Rules 2011)

In April 2011 the Electronic Service Delivery Rules to the Information Technology Act[88] were notified. The Rules enable state governments to deliver public services through electronically enabled kiosks and other electronic service delivery mechanisms. In doing so the Rules maintain that state governments must create a system for the electronic delivery of services, and the appropriate authorities must create and maintain repositories of electronically signed records. Aspects of the Rules that pertain to privacy include:

- *Encryption of sensitive records*: The Rules allow the appropriate government to determine the manner of encryption and confidentiality for sensitive electronic records.[89]

- *Data Retention*: All authorities that issue a license, permit, certificate etc must create a repository of the signed records and retain these records. The manner that these documents must be retained will be established by the appropriate government.[90] Additionally, the appropriate government has the authority to direct any service provider to retain records of the transactions, receipts, and vouchers collected from payments.[91]

- *Reactive Disclosure:* Records maintained by Service Providers must be disclosed to any agency or person nominated by the appropriate government for inspection and audit.[92]

- *Security Procedures:* The appropriate government must specify the security, management, and storage procedures for maintenance of electronic data, information, applications etc. stored in the repository [93]

- *Changes to records:* All changes made to records in the repository, including updating or correcting the record, must be signed by the person authorized to make the changes along with time stamps of the original creation and modification. [94]

- *Confidentiality of Data:* All service providers etc. must submit a declaration stating that the data of every individual transaction and citizen will be protected. If unauthorized disclosure without consent takes place, the service provider will be debarred from providing that service any further.[95]

- *Missing Safeguards:*
    - Interoperability
    - Distinct categories of information
    - Breach notification
    - Anonymization/obfuscation and deletion policies
    - Accountability for accuracy of data
    - Appropriate uses of databases
    - Individual access, updation and control of personal information

Proposed Legislation

The Unique Identification Bill, 2010

The Unique Identification Bill[96] was proposed to Parliament in 2010. If passed, the Bill will legalize the issuance of a 12 digit unique number (Aadhaar number) based on an individual's biometric data. The Aadhaar number along with an individual's biometrics will become a form of authentication in transactions. Along with establishing the UID Authority, the Bill establishes enrolling agencies, registrars, and a review committee. Additionally, the Bill legalizes the creation of the Central Identities Data Repository – a centralized database that will contain both Aadhaar numbers and the corresponding biometric information of enrolled residents. Aspects of the Bill that are relevant to privacy include:

- *Sharing:* With consent, the Authority will be responsible for sharing the information of Aadhaar number holders with the relevant businesses engaged in delivery of public benefits and public services.[97]
- *Security:* The Authority will be responsible for developing security protocols to follow by registers and enrolling agencies.[98] The Authority will ensure the security and confidentiality of identity information and authentication records. This includes protection against unauthorized access, use, or disclosure.[99]
- *Redress:* The Authority will be responsible for establishing facilitation centers and grievance redress mechanisms.[100]
- *Unlawful Disclosure:* The Authority, officer, employee, or agency who maintains the Central Identities Data Repository will not reveal any information stored in the Central Identities Repository. This standard is not withstanding to any other law in force or as otherwise provided for under the Act.[101]
- *Lawful disclosure:* Information is permitted to be disclosed under the Act through a court order or disclosed in the interests of national security upon an order made by any officer not below the rank of Joint Secretary.[102]
- *Proactive Discovery:* The Authority will be responsible for calling for information and records, conducting inspections, and audit of information from the Central Identities Data Repository, Registrars, enrolling agencies, and other agencies appointed under the Act.[103]
- *Accuracy:* The Aadhaar number holder will be responsible for ensuring that his/her demographic information is correct, and must request the Authority to make the necessary changes.[104]
- *Data Retention:* The Authority will retain the details of every transaction (request for authentication and response) for a period of time and in a manner that will be specified by regulations. Every Aadhaar number holder will be entitled to obtain these details from the Authority.[105]
- *Penalties:* The following are offenses under the Act. Individuals who commit these offenses are held criminally liable: impersonation at the time of enrollment, impersonation of an Aadhaar number holder, disclosure of identity information, unauthorized access to the Central Identities Data Repository, tampering of data in the Central Identities Data Repository, manipulation of biometric information.[106]
- *Investigation*: A police officer not below the rank of Inspector Police will have the e power to investigate any offense committed under the Act.[107]

- *Maintenance:* The Central Identities Data Repository is permitted to be maintained by multiple entities.[108] These entities will be appointed by the Authority.[109]
- *Collection*: The Authority will be responsible for developing procedure for the collection of demographic and biometric information.[110]
- *Authentication:* The Authority will be responsible for developing procedure for the authentication of Aadhaar numbers.[111]
- *Deletion*: The Authority will be responsible for the deletion of an Aadhaar number.[112]
- *Use:* The Authority will determine the use and applicability of the Aadhaar number for the delivery of benefits and services.[113]
- *Reactive Disclosure*: All individuals who wish to obtain an Aadhaar number must provide his/her demographic and biometric information.[114] Individuals will not be required to provide information pertaining to their race, religion, case, tribe, ethnicity, language, income or health[115], but through regulation the Authority is enabled to specify demographic and biometric information for enrollment[116]. Individuals, who have enrolled for a UID number, may be required to update their demographic and biometric information by the Authority.[117]

There are many aspects of the project design that raise privacy and security concerns including: iinappropriate use of data for tracking, inadequate privacy safeguards, unwarranted data retention, lack of accountability to security of information for all actors, lack of rollback and ombudsman office, insecure project architecture, insecure use of biometrics, and the unnecessary storage of transactional data.

DNA Profiling Bill 2007

The Draft DNA Profiling Bill[118] was piloted by the Center for DNA Fingerprinting and Diagnostics.[119] The DNA Profiling Bill was first introduced in 2007. In 2012 a new version of the Bill was released to the public and is pending. Both the DNA Profiling Bill 22007 & 2012 look to legalize the collection and analysis of DNA samples for forensic purposes. The following aspects of the Bills pertain to the privacy:

- *Collection:* The schedule of the Bill lists the offenses and situations for which the collection of DNA is permitted.[120]
- *Privacy Principles*: The DNA Profiling Board is enabled to recommend privacy protection statutes, regulations, and practices concerning: use and dissemination, accuracy, security, and confidentiality, and destruction of DNA information.[121]
- *Storage and retention:*[122] The Bill provides for the complete storage of DNA samples of: volunteers, suspects, victims, offenders, children (with parental consent), and convicted persons.
- *Access:* The Data Bank Manager is given sole discretion as to who may have access to the DNA database, including persons given access for training purposes.[123]
- *Offenses:* Unauthorized access, disclosure, destruction, alterations, and tampering, is penalized under the Bill.[124]
- *Redress*: The Bill provides no redress mechanism to an individual whose DNA was illegally used or collected. Furthermore, only the Central Government or DNA Profiling Board are enabled to bring complaints to the courts.[125]
- *Access by law enforcement agencies*: The Bill currently allows for the DNA Profiling Board to grant law enforcement agencies access to DNA profiles.[126]

- *Contamination of DNA samples:* Laboratories are held responsible for "minimizing the contamination of DNA."[127]
- *Indices held by DNA Banks:* The DNA data bank sets up indices that hold DNA identification records and DNA analysis from: crime scenes, suspects, offenders, missing persons, unknown deceased persons, volunteers and such other indexes as specified by regulations.[128]
- *Communicating of DNA Profile with Foreign States*: With the approval of the Central Government, the sharing of DNA profiles with Foreign States.[129]
- *Definition of DNA:* The introduction of the Bill states that with DNA it is possible to determine if the source of origin of one body substance is identical, and establish the relationship between the two without any doubt. This is an incorrect statement as more than one individual can have the same DNA profile as another individual, and system errors when analyzing and identifying DNA can take place.
- *Comparison of Profiles*: Individual DNA profiles that have been collected will be compared with the stored profiles on the database in order to check if an individual is already on the database.[130] The Bill also requires identifying information to be stored with the DNA profile collected from an individual[131] This increases the chance for false matches to occur between newly added individuals' DNA profiles and stored individuals' DNA profiles. Furthermore, if the DNA database is going to be useful in solving crimes, identifying information beyond a DNA profile will need to be stored to allow for criminals to be traced and identified. The amount of information that will actually need to be stored for the database to be useful poses as a threat to privacy.
- *DNA to be used in Civil Disputes:* The Schedule hold that the DNA data bank can store profiles used in Civil Disputes and other Civil Matters[132] Including DNA profiles collected for civil purposes on the DNA database will create privacy concerns and add to the number of profiles on the database - thus increasing the possibility for false matches.
- *Establishment of identity:* The Schedule includes "Issues relating to establishment of individual identity". Allowing the database to be used to establish identity (rather than being restricted to searching for matches with crime scene DNA) allows for potential abuses.
- *Removal of profiles:* The DNA profiles of persons who are acquitted of an offense.[133] This is a positive step to protecting privacy.

Missing safeguards:

- *Individual Access:* Individuals should have the right to ask the police for any of their own details held on police databases. This will allow an individual to know if their data is being held against the law[134].
- *Identity:* "Identity" and how "identifying" information can be used should be clearly defined. Furthermore, it is important to ensure that no other information (like an identity number) that would allow for function creep is included in the DNA data base.[135]
- *Restricted Access:* The DNA database should be restricted to the identification of a perpetrator of a specified criminal offense, and consent or a court order must be sought for any other use of the database for identification purposes.
- *Destruction of profiles:* A requirement for the destruction of individuals' DNA samples (usually mouth swabs) stored in laboratories should be provided for in the Bill.

- *Probability of error published*: With a population the size of India, the number of these false matches could be very high. The DNA board should take this probability for error into consideration and publish researched statistics on how many false matches they expect to occur purely by chance, based on the numbers of profiles they expect to store under the proposed criteria for entry and removal of profiles.
- *Restricted Use:* The proposed DNA database should be restricted to use for criminal investigations and the identification of body parts only: civil uses should be excluded from the Bill. Any missing persons' or elimination databases should be entirely separate from the proposed criminal DNA database.
- *Transparency:* The DNA board should be transparent about (i) what identifying information will be stored from individuals to enable them to be tracked in the event of a 'cold hit' between their DNA profile and a crime scene DNA profile; (ii) the proposed process for removals of innocent persons' records; (iii) the proposed rules for elimination databases, including police officers and laboratory personnel.

Case Laws

Passports Act 1967

Mr. Sarella Vara Prasada vs Ministry of External Affairs, CIC, 2011[136]

In this case, the appellant, Mr. Sarella Vara Prasada by way of a RTI Application sought information regarding the passport details of Rotte Bujji's age, marital status and her parent's name. The PIO (Passport Information Officer) as well as the FAA (First Appellate Authority), on First Appeal.

The FAA upheld the PIO's ruling; denying disclosure of the information under Section 8 (1) (j) of the RTI Act on the basis that "disclosure of personal information of a third party might cause invasion of the privacy of the third party".

On the basis of the facts of the case and studying the exemption provided by law under Section 8 (1) (j) of the Act, the CIC observed and held that the "term "personal" to be an attribute which applies to an individual and not to an Institution or a Corporate. From this it flows that 'personal' cannot be related to Institutions, organizations or corporates. Hence Section 8 (1) (j) cannot be applied when the information concerns institutions, organizations or corporates". The CIC also observed that "the phrase "disclosure" which has no relationship to any public activity or interest, means that the information must have been given in the course of a Public Activity".

On the premise that when a State routinely obtains information from the Citizens, this information is in relationship to a public activity – the CIC held that this does not constitute an intrusion on privacy. The PIO was directed to provide the necessary information to the Appellant.

Mr. G. Gururaja Rao vs Ministry of External Affairs, CIC, 2012[137]

In this case, Privacy was not deemed to be protected under Section 8(1) (j) of the RTI Act. The CIC was of the opinion and ruled similarly that "a passport issued by a public/government servant is itself is a public document, as it will have to be produced at anytime and anywhere for scrutiny. Therefore, a passport issued to a public servant cannot be called a personal document, as it will be meant for other purposes as may be required in the circumstances". Therefore, the information sought cannot not deemed as privileged and classified under section 8 (1) (j) of the Right to Information Act, 2005.

Shri Durgesh Vijayvargiya vs Ministry of External Affairs, CIC, 2012[138]

The Appellant, by way of a RTI Application, requested information with respect to the addresses of certain persons as well as the validity of their passports, details of fresh passport issued if any, details of present residence along with visa information, etc.

The CIC observed that "The State has no right to invade the privacy of an individual. There are some extraordinary situations where the State may be allowed to invade the privacy of a Citizen. In those circumstances special provisions of the law apply;- usually with certain safeguards. Therefore where the State routinely obtains information from Citizens, this information is in relationship to a public activity and will not be an intrusion on privacy. The Appeal was allowed. The exemption under the relevant Sec 8(1) (j), could not be sought.

Census Act, 1948

P.C. Wadhwa vs Central Information Commission, Punjab & Haryana High Court, 2009[139]

This case represents an appeal filed by the Appellant against the order of the CIS, whereby he was prevented from being given access to information regarding the religion of certain leaders on the basis that "no person had the right to inspect any book, register or record made by a Census Officer in the discharge of his duty as such or any item under Section 10 of the Census Act".

The moot point being that for preparing census, facts are collected from individuals in a household, which are confidential in nature and are to be used only for statistical purposes and no else.

The CIC taking the facts of the case and request of the Appellant into account, dismissed his appeal, taking into consideration the provision under Section 8(1) of the RTI Act read along with Section 15 of the Census Act, which states that:

"No person shall have a right to inspect any book, register or record made by a census-officer in the discharge of his duty as such, or any schedule delivered under section 10, and notwithstanding anything to the contrary in the Indian Evidence Act, 1872, no entry in any such book, register, record or schedule shall be admissible as evidence in any civil proceeding whatsoever or in any criminal proceeding other than a prosecution under this Act or any other law for any act or omission which constitutes an offence under this Act"

This stipulates that unless it is for a larger public good, personal information shall not be made know to the public. This clearly reflects that census information which is confidential and privileged, is protected under the privacy umbrella and no exception can sought, without showing a dire public/social need in the larger interests of society or country.

Citizenship Act, 1955

Ms. K Sharada vs Ministry of External Affairs, CIC, 2009[140]

Ms. Sharada by way of a RTI Application filed with the CPIO (Central Public Information Officer) in 2008 sought information/copies of all documents submitted by Mr. Suhas Chakma at the time of applying for his Passport; including proof of date of birth and Citizenship document.

Her contention was on the basis that Mr. Chakma is not known to have any birth certificate. Nor is he known to have applied for a Citizenship certificate. No proof exists of his having Indian nationality either by birth or by naturalization. Meanwhile, he avails of all the benefits of Indian citizenship such as a passport, ration card and voting rights and even receives additional benefits through an ST certificate.

Further, Sharada maintained that the information was already in the public domain since Mr.

Chakma had to submit details pertaining to his nationality and date of birth while applying at the JNU; also that there were instances of people applying for admission/employment/positions on the basis of forged and false documents. It was therefore in the interests of transparency and also to put a restraint on the irregularities that this information must be disclosed.

The Appellant, further pointed out that the RTI application was filed pursuant to a complaint registered against Mr. Suhas Chakma, with the Foreigners Regional Registration Office on the grounds that despite being a Bangladeshi national he had registered himself as an Indian citizen through fabricated documents and certificates. Along with the appeal, she submitted three judgments reflecting the concern of the Delhi High Court on the issue of detection deportation of illegal migrants from Bangladesh to substantiate her submissions on larger public interest concerns.

The CPIO dismissed the Application on the basis of the provision in Section 8(1) (j) of the RTI Act, whereby third party information is privileged and protected.

The CIC, taking all facts into consideration- maintained that public interest does dominate any individual interest and taking into account the flow of illegal immigrants from a national safety and security perspective, the CIC ruled that there is a need for transparency in the functioning and mechanism of the Ministry of External Affairs. The CPIO was directed to furnish details of Mr. Suhas's passport documents- he cannot take protection under the Privacy protection clause of Section 8(1) (j) of the RTI Act.

This is a clearly a case where public safety and national security has prevailed over privacy concerns of an individual.

Implementation

Identity

Ration Cards

In India the ration card is a government issued identity that allows citizens to obtain governmental benefits like food grains and petrol through the public distribution system.[141] In addition to being used for access to governmental benefits, ration cards are often used as supporting proof of identification. As many news items have pointed out – for the poor, ration cards are the main form of identity that they have.[142] Because of the widespread use of ration cards the Indian government is faced with fraudulent use of ration cards in the PDS system. The Government is also faced with errors in the data entered into the system, which is a privacy concern as individuals have no assurance that their data is accurate and is not being misused. The Government and individual States over the years have taken many steps to eliminate the fraudulent use ration cards. For example some States have started using hologram-enabled ration cards and smart cards.[143] In June 2011 the GOI issued a statement detailing its plans to replace the entire system of paper based ration cards with smart cards. These smart cards will be based on biometrics, and will digitize individuals ration data.[144] The ration card has no supporting legislation.

PAN Cards

The PAN card is issued by the Income Tax Authority and is required as proof of identity in most financial transactions. In practice, privacy concerns arising from the issuance and use of the PAN include a) the type and amount of information that the tax department can collect/compile about an individual from use of the number, b) who (which governmental departments) can access to the information generated from the use of the number and how can this information be used c) what steps can an individual take if their number or card is stolen. Many of these concerns are relevant in the Indian context as the scope of collection and compilation of information by the Tax Authority is expanding. For example, The Central Information Branch, the intelligence wing of the Central Board of Direct taxes,145 has recently put in place "software that already has extensive information on taxpayers mapped to their respective PAN cards"146 Similarly, in 2006, the then Finance Minister Chidambaram, proposed a plan to issue biometric PAN cards which "would have carried the I-T assesses' fingerprints (two from each hand) and the face." In 2011, the Finance Ministry announced measures to streamline the financial information provided by third parties – such as banks and mutual fund companies - to the CBDT to facilitate smoother and faster access to information about persons.[147] In August 2011, the IBA (the Indian Banks' Association) representing "more than 160 Indian and foreign banks operating in the country" agreed to provide access to banks' data bases with the Central Board of direct taxes – supposedly in order to check the accumulation of black money. This would give tax authorities "a 360 degree view of the taxpayer." [148]

Election Cards

Accurate and consistent data collection, data storage, and data access are privacy concerns that arise when preparing, storing, and sharing information on electoral rolls. In August 1993 the ECI decided to issue Elector's Photo Identity Cards (EPIC) to all voters in India to ensure their correct identification and prevent impersonation.[149] The EPIC contains the following details - the name of the elector, relation's name, date of birth, gender, address, and the photograph of the individual. In addition, every EPIC is fixed with a security hologram and has a unique 10 character alphanumeric string called the EPIC Number.[150] The EPIC card and subsequent database faces many challenges including: integration - each EPIC database is maintained in relation languages; interoperability - EPIC databases are maintained at the level of each constituency, thus voters are required to obtain fresh ID cards in each new constituency that they shifted to. Inadequate co-ordination within the election commission has led to voters maintaining separate voter IDs in different constituencies that they transferred to. In addition, the database of voters and the database of photographs are frequently maintained separately and are imperfectly linked. In order to streamline the process and consolidate the disaggregated data, in February 2008, the ECI centralized its databases and directed the Electoral Database and the photo database to be centrally maintained in one database for the entire State.151 Another important source of concern from the privacy perspective is the degree to which the enrollment process for election cards is conducted by contracted agencies. Apart from contractual terms which require an agency to turn over all data collected to the Election Commission and not retain anything beyond the period of the contract, there are no safeguards and standards that the ECI mandates contracted agencies to observe. An important contribution to privacy, in this context, would be sanctions meant to govern agencies whom the ECI contracts to perform the tasks of enrollment and issuance of ID cards.

National Identity Cards

The Multi Purpose Identification Card (MNIC), proposed in 1999, was the first attempt by the Indian Government to create a single national identity card.[152] The MNIC was designed as a smart card that functioned off of the SCOSTA standard – an indigenous identification technology based on open standards, and secured with asymmetric and symmetric key cryptography to protect privacy. It was planned that the card would carry information like a 16 digit Unique National Identity Number, an individual's name, address, date of birth, fingerprint, etc. The project proposed creating a National Population Register to hold the details of 'usual residents'.[153] Information was to be collected from individuals by census enumerators who obtained 14 different categories of data along with the photographs, finger prints and iris's of individuals.154 The Government also envisioned creating a National Population Register (NPR) to hold the details of individuals. At the time identified legal issues with the scheme included: iinaccuracies in collection, data theft/security, data correction issues, function creep, lack of redressal mechanisms, and lack of judicial safeguards.[155] Alongside the MNIC card the Government envisioned establishing a UID number separate from the MNIC initiative. The UID database was first envisioned as being a database created for the verification of individuals and for establishing their credibility. It was to be based on the voter list of the Election Commission of India and also linked to major database holders like the MoRD, PDS, ECI, and RGI.156 Eventually, the Government decided to abandon the issuing of the MNIC card, but still continued with the creation of the NPR database and merge it with the UID database. It is envisioned that the data collected for the NPR database will be sent to the UIDAI for de-duplication and merged onto the UID database, and identity cards created under the NPR will hold the UID number of that individual. Currently, the NPR proposes to digitize the demographic data captured in the 2010 census operations, and collect the biometrics of individual age five and up. The process for data capture will be house to house canvassing, digitization of data, storage of data in a database, and biometric collection.[157]

Today, the UID is in the process of being connected to a number of databases, cards, and services including the voter ID card158, citizen email addresses159, criminal records, and PAN cards. 160 States are in the process of connecting services like the Public Distribution System, LPG distribution, Kerosene disbursal, Government pension schemes, Janani Suraksha Yojana, Government Scholarships, Financial Inclusion, Kisan Credit Cards (KCCs) and MGNREGS wage disbursal to an individual's UID number. The extent to which databases and services are being connected to the UID is a privacy concern as data mining, data collation, and tracking are made possible. Furthermore, the UID has faced problems with accurate collection and verification of data.[161] Concerns have also been raised in regards to the accountability of the UIDAI, especially because the authority currently does not fall under the ambit of the Right to Information Act.[162]

DNA Databases in India

DNA collection and testing is taking place in many states in India. For instance, in Pune the army is currently considering creating DNA profiles of troops who are involved in hazardous tasks in order to help identify bodies mutilated beyond recognition.[163] In December 2010 a judge in the High Court of New Delhi ordered DNA testing on a senior congress member to determine if his child was really his child.[164] Also in December 2010 a news article announced the establishment of the first DNA profiling databank in Nehru Nagar.[165] Additionally, DNA has been used to identify criminals. For instance, in the Tandoor Murder, DNA testing was used to reveal the identity of the culprit.[166] India hosts both private and public DNA labs. Public labs are sponsored by the Government, and use DNA purely for forensic purposes. For example The Center for DNA Fingerprinting and Diagnostics (CDFD) located in Hyderabad is sponsored by the Department of Biotechnology and Ministry of Science. CDFD runs DNA testing for the establishment of parentage, identification of mutilated remains, establishment of biological relationships for immigration, organ transplantation, property inheritance cases, identification of missing children and child swapping in hospitals, identification of rapist in rape cases, identification in murder case Cases are only accepted by CDFD if they are referred by law enforcement agencies or by a court of law. Only an officer of the rank, inspector of police or above may forward DNA cases to CDFD. Copies of DNA report are released to individuals if they are able to prove needed interest in the case through a notarized affidavit[167]. In 2010 CDFD received 100 cases from law enforcing agencies. Additionally, in 2010 CDFD was given rupees eighteen lakhs thirty nine thousand five hundred and forty five from the Government of India towards DNA fingerprinting services.[168] Examples of private DNA labs include DNA labs India[169] and Truth Labs. DNA labs India runs paternity testing, forensic testing, prenatal testing, and genetic testing. Truth Labs is a private lab that provides legal services directly, without a court or police order. [170] DNA facilities are also becoming more widespread in India through the establishment of multipurpose forensic laboratories accessible to law enforcement and intelligence agencies. For instance in Assam, Mumbai, and Hyderabad new forensic laboratories with DNA testing facilities have recently been set up. [171]

Identity Theft

Identity theft is rampant in India, and with the growth of information communication technology it has increased exponentially. For example, the Cisco World Technology Report shows that at least 32% college students surveyed in India are victims of identity theft.[172]

The government is aware of the threats to privacy, and the need for adequate data protection laws to protect against identity theft. One of the main reason identity theft is such a huge problem and a threat in India is because of the number of identities that exist - increasing the probability of any of them being replicated.173 For example, in 2011, a Delhi University law student was alleged to have been stalking and threatening a woman online, and while doing so had created fake profiles of the woman. Though the woman initially filed a complaint, she withdrew her complaint after the accused apologized and promise never to repeat such kind of acts. Despite this promise, the accused continued to impersonate the woman on social networking websites, and made contact with her friends. A case under Section 66-A of the Information Technology Act was instituted and the victim stated in her complaint that, "she is a victim of cyber stalking and identity theft which has created grave problems for her and her family".174 Similarly in 2010, in Mumbai, two cases of sending 'masked SMS' were reported. The perpetrators of the crime were using websites which enabled them to send text messages to and from any mobile phone for a fee of $10. In the article, an IT expert was quoted saying that the law in India "is still inadequate to handle such innovative mobile spoofing." [175]

In a unique case filed in 2010, the Bharatiya Janata Party accused the ruling party of identity theft. A notice served by the BJP, alleges that Congress had covertly hosted a website with the domain name www.bjp.com. This website redirects the visitor to the Congress website. The official domain name of BJP is www.bjp.org.[176] These examples demonstrate that despite having laws in place, implementation of the regulations is a challenge.

E-Governance

National E-Governance Plan (NeGP)

In May 2006, the Indian government approved the National E-Governance Plan (NeGP), which was conceptualized as a comprehensive approach towards making government services available to people in their specific localities while meeting goals of efficiency, transparency, reliability, and affordability. Broadly speaking, the infrastructure, governance, and implementation of the National E-Governance plan has many privacy implications. For example, it is proposed to create State Data Centres in order to allow States to consolidate services. The State Data Centre will facilitate services such as: Citizen Information/Services Portal, State Intranet Portal, Disaster Recovery, Remote Management and Service Integration etc. The Department of Information and Technology (DIT) has created guidelines for the Technical and Financial Support for Establishment of State Data Centres[177] Among other things, the guidelines envision a data retention plan that would be formulated by the State,[178] mechanisms that ensure physical and network security, and puts inplace security audits for every six months. [179] The DIT has also created a best practices and guidelines document outlining best practices in data security that the State must develop and enforce when running a State Data Center. Broadly, the guidelines place the obligation on the State to develop and implement trust and identity management policies, security posture assessments, data privacy polices, ensure confidentiality and monitor access to data, and implement disaster recovery and business continuity plans.[180]

The NeGP also envisions the development of Common Services Centers (CSC). CSC's are computer resource centers designed to provide an accessible facility for the delivery of e-services in rural and remote areas. Services that will be provided at CSC's include information relating to health, education, agriculture, and employment. Individuals will also be able to complete payments like NREGA, utility payments, and access online banking services. As envisioned, the project has a three tiered governance framework that includes 1. State Designated Agencies involved in monitoring and supervising the CSC at the state level. 2. A Service Centre Agency – meant to provide the required investment budget and the functional specifications for the CSC 3. Village Level Entrepreneur in charge of running daily operations at the CSC.[181] An example of how CSC's could be used can be see through DITs proposal to leverage the CSC network for the carrying out of the NPR project by capturing and entering data at centers.[182]

Public Information Infrastructure[183]

In 2009, Prime Minister M. Singh appointed Sam Pitroda to the cabinet-level position of Adviser to the Prime Minister for Public Information Infrastructure[184] and Innovations, tasked with developing a unified policy for information standards and practices incorporating both intra-government affairs and citizens' services. In June 2010, Mr. Pitroda's office uploaded an online a slide presentation on "Strengthening Democracy and Governance: Public Information Infrastructure." The presentation provides a basic overview of his proposal for a robust information system. Included in the scheme is the development of a national repository of information on people, including citizenship, resident, and household data; places, including villages, towns, streets, schools, hospitals, government offices, factories, officers, residences, stations, mines, minerals, dams, plants, rivers, parks, forests, farms, etc.; and programs and other government offices, such as the National Rural Employment Guarantee Scheme, the Public Distribution System, girl child benefit schemes, pensions, the judiciary, police and prisons, treasuries, land records, universalize elementary education, and the National Rural Health mission, among others. Applications hosted on the PII will include a shared Geographic Information System (GIS) for the Survey of India; the National Disaster Management program; the Urban Ministry; the Departments of Space, Security, Environment, Health, and Rural Development; the Planning Commission; as well as private enterprises. Data from these entities will be publicly available on a single portal accessible by a variety of clients, including PCs and mobile phones. The portal will also incorporate applications, communities, mash-ups, and allow for a variety of analyses on data including including survey, remote sensing data, census, education, and health data, as well as forest, land use and groundwater data.[185]

National Data Sharing and Accessibility Policy

This policy[186] was approved by the Union Cabinet on February 9th 2012. The policy is a broad framework that applies to all data and information created, generated, collected and archived using public funds provided by the Government of India for the purposes of enabling *ready access to valuable data is essential for a number of decisions and tasks including development planning, controlling disasters, and national security.* The policy focuses on integrating all governmental databases to facilitate governmental access to information, and is based off of principles like: Openness, Flexibility, Transparency, Legal Conformity, Protection of Intellectual Property, Formal Responsibility, Professionalism, Standards, Interoperability, Quality, Security, Efficiency, Accountability, Sustainability, and Privacy. A data warehouse will be set up to house current and historical data so that this information in is one place.

The policy divides types of data between shareable data and non shareable data, and creates multiple levels of access to data including: open access, registered access, and restricted access. It is also envisioned that all departments will prepare a list of data that is not to be shared within six months of notification. This list will be determined using the provisions in the RTI Act. All other data sets will be considered safe to be opened to the public. Meta Data would also be provided which would allow people to know what data is available Different steps for implementation of the scheme have been outlined such as making data available on an “as-is where-is' basis, and requiring that all valuable data sets be uploaded by the end of three months, all data sets be uploaded by the end of this year, and after that – be updated on a quarterly basis etc. Privacy concerns associated with the policy include possibility of function creep and misuse of data from the integration and sharing of data across governmental departments. Furthermore, the lack of clarity over which authority will be responsible for allowing or restricting access to data creates a vulnerability in the security of the policy.

National Knowledge Commission recommendations

In June 2005, Prime Minister M. Singh constituted the National Knowledge Commission (NKC), an advisory body to the Office of the Prime Minister, with the mandate to recommend[187] policy reforms in the areas of “access to knowledge, creation and preservation of knowledge systems, and dissemination of knowledge and better knowledge services.” After three years of review, the NKC issued a series of reports in the “National Knowledge Commission Final Report 2006-2009.” In its Final Report, the NKC made two recommendations particularly relevant to implementing open government data in India. First, the NKC “recommended the establishment of a high-end National Knowledge Network connecting all … knowledge institutions in various fields and at various locations throughout the country, through an electronic digital broadband network with gigabit capacity". Second, the NKC proposed that the government create a series of “national web based portals on certain key sectors such as Water, Energy, Environment, Teachers, Biodiversity, Health, Agriculture, Employment, Citizens Rights etc. that would serve as a single window for information on the given sector for all stakeholders . The NKC also recommended that government departments should make data sets they have available in a digital format. It is unclear to what extent this recommendation has been followed.

Private Public Partnerships

As governments move towards implementing e-governance projects, they engage with private entities through Public Private Partnerships (PPPs) to help in the design, implementation, and delivery of services. Though these businesses help in designing and implementing various projects, privacy becomes a concern when the private sector collects personal information, as often the information is protected only through contract. An example of how PPP's challenge privacy can be seen through the project developed between Tata Consultancy and the Indian Government. In October 2008, Tata Consultancy Services a prominent software services company in India was awarded a Rupees 1000 crore project to “provide passport-related services to Indian citizens in a speedy, convenient and transparent manner.”[188] In the absence of anything in the Passport Act prohibiting the outsourcing of essential functions, the task of safeguarding of citizens’ privacy falls to the domain of contract law – assuming the contract between the state and the company contained a standard confidentiality clause - and the limited provisions of the IT Act dealing with data protection. The contractual option does not provide reliable privacy safeguard since it is only enforceable by the state against the private company and the state has had, at best, a patchy record has of defending its contractual rights against private companies. The following extract, from a newspaper account about the outsourcing of biometric data collection illustrates the fluidity with which data sharing across databases occurs today between governments and contracted companies.*“The project, conceived by WFP in 2007, was started a year ago with Hyderabad-based 4G Identity Solutions Pvt. Ltd as technology partner. Using its 125-member team, the firm digitized old ration card registers and mapped these with the database of the 1997 BPL survey and 2002 household survey. The gram panchayat target beneficiary database was then transferred to some 6,000 enrollment stations in 2,445 villages, 41 wards and three urban local bodies where people queued up to get their biographic and biometric data recorded. Data from enrollment stations were sent to the 4G data centre for aggregation where de-duplication was done using a multi-modal biometric engine to check for fake enrollments. A final database of unique card holders was generated and stored in a centralized citizen database. Rural households have been given laminated bar-coded ration cards and coupons since point-of-sale machines cannot be used in villages, several still without electricity.”* Indian Express, August 2003[189] though PPP's can greatly help in the delivery and development of infrastructure and services, it is important that the project is regulated by more than just a contract in order to protect the privacy of the data.[190]

State wide E-Governance infrastructure:

Increasingly, various states have taken initiatives to transform entire government services and infrastructure to be digital. For instance, in 2012 the State of Kerala announced that it would soon making the state 'fully digital'. This will include providing every citizen with an e-mail ID that would be based on their UID number, thus allowing all communications, transactions, and applications between the government and the citizen would take place through e-mail. Pensions and scholarships would be distributed to entitled individuals via the banks, and all government files will be converted to the digital mode.191 The underlying architecture to these plans include the establishment of a department wide network which will connect governmental departments and public offices. This network will allow all connected departments to access data, voice, and video services. The department wide network will then be connected to the Kerala State Wide Area Network.192 Questions related to privacy that the initiative raises include: how will the State ensure that citizens email connections are secure and not accessible by different government departments, how will the state ensure accuracy in converting documents to the digital form, and what security measures will be put in place to ensure that as governmental databases are created – unauthorized access, collation, data mining, and tracking do not take place.

MCA21:

In 2006 the Ministry of Corporate Affairs (MCA), Government of India, began to put in place plans for a project known as MCA21. [193] In 2012, the Government has pushed to finish the project. The project aims to convert processes, transactions, and legal requirements found under the Companies Act to the digital. The objective of the service is to allow for transparency and tracking of corporate activities in order to identify and resolve suspicious and fraudulent corporate transactions.[194] Components of the project that impact privacy and that are still unclear include: the extent of information that will be collected, how this information will be stored/secured/deleted, and who will have access to the information.

TAGUP[195]

In February 2011 the Unique Identification Authority of India (UIDAI) Chairman, Nandan Nilekani, submitted a seven-member group's report detailing specific recommendations for IT-intensive projects such as the Tax Information Network (TIN), New Pension Scheme (NPS), National Treasury Management Agency (NTMA), Expenditure Information Network (EIN) and Goods and Service Tax (GST). Among the recommendations, the TAGUP has envisioned that to handle all aspects of IT systems for governmental projects, a National Information Utilities (NIU) will be put in place. The report calls for the use of open data, open standards, using open source, and envisions an interoperable system. Among other things, the report recommends that designers of e-gov projects should take pro-active actions in deciding what information to share publicly, as most information held by the government is required to be shared under the RTI act. The report also broadly recognizes the need to protect the privacy of data entered into the system and recommends guidelines that could be included in a privacy legislation. The recommended guidelines include the following:

- *Solution architecture and privacy*: A privacy legislation should put in place rules that can be implemented and incorporated into IT systems and projects from the very start of the project.[196]
- *Personal Identifiable Information*: Personal Identifiable information should be stored separate from other data and in an encrypted form. Separate access controls should be defined for personal identifiable information, and unauthorized access should be penalized. [197]
- *Anonymization of Data:* Data should be anonymized when released to the public. The method of anonymization should follow the logic of k-anonymity – where each record is indistinguishable from k-1 other records.[198]
- *Data Retention:* Data retention policies should be well defined. If records are needed to be retained for long periods of time, personal identifiable information should be scrubbed from logs after a pre-defined time. Individuals should be able to access personal data stored in the IT system after authenticating their identity.[199]
- *Balancing the Right to Privacy with Public Interest:* In the case of national security, economic offenses, tax evasion, and other specified circumstances, Government agencies will need to access or share data. This access should be permitted, but should be carefully regulated by a data protection regime.

Bhoomi

Bhoomi[200] is an e-governance initiative that works to computerize land records. The project was started in Karnataka and designed by the National Informatics Centre (NIC). It focuses on enhancing the delivery and management of land records. The objective of BHOOMI is to reduce the discretion of public officials by allowing for individuals to issue a mutation request online. This allows any individual (farmer & non farmers) to access the database. Individuals who apply online can obtain a printed copy of the RTC by providing the name of the owner or plot number at computerized land record kiosks in taluk offices. A second computer screen faces the clients to enable them to see the transaction being performed. A farmer can check the status of a mutation application on Touch Screen Kiosks. If the revenue inspector does not complete the mutation within 45 days, an individual can approach a senior officer with their grievance.

Important features of the project related to privacy:

- *Security*: The Bio-logon metrics authenticates various users on the Bhoomi software on the basis of fingerprints. This measure ensures that no one can hack into the system by imitating other users.
- *Authenticity*: Original mutation orders of the revenue inspector (who is the authorized person to pass orders in the mutations in the field) and notices served on interested parties are scanned to ensure authenticity and accuracy.
- *Access:* The Bhoomi system is open to all individuals who have a 'revenue number.' The implication of this is that persons who are not the owners of the land are able to collect RTC papers from a Bhoomi Kiosk by quoting a 'revenue no.' Though access is important to facilitate the transparency that the system hopes to achieve, it is possible for this information to be misused.
- *Transparency:* The system makes all division, buying, and selling of land transparent to the public. This gives individuals the ability to follow the transactions of bureaucrats and public officials and monitor the amount of their accumulated wealth. On the other hand, because of the transparency of the system privacy infringing circumstances can come about. For example, Banks who are performing 'due diligence' checks have the ability to access client land records without obtaining prior consent.

Recommendations

Broadly speaking, it is undeniable that e-governance schemes are beneficial in many ways. How the ecosystem of the schemes are designed, who the scheme should apply to, what should the scheme enable, what privacy measures should be put in place, and to what degree do residents and citizens have control over the information that is collected are questions that need to be answered. At the basic level it is important that any scheme implemented by the Government of India should inhibit the merging of databases, information, or project goals from other government initiatives. Furthermore, it is important that there are strong legally backed data protection standards in place as every identification scheme will include the formation of databases that hold highly sensitive information. From the above examples it is clear many of the governmental databases in India face privacy risks such as: inaccurate data, incomplete data, inappropriate disclosure of data, inappropriate access to data, and inappropriate security over data. Below is a list of recommendations[201] concerning privacy and government databases.

- **Citizen-State relationships and privacy standards**
  Government databases foster different types of relationships between the state and its citizenry. For instance: User databases, service providing databases, and information providing databases. Each one these relationships requires a different level of privacy. Thus, it is important to identify the type of relationship that the database will foster in order to determine what type of privacy model to implement.
- **Personal vs. personal sensitive, private data vs. Non-private data, and public vs. non-public data categories**
  Data in government databases requires varying degrees of privacy safeguards. The division of personal information vs. non personal information etc. creates distinct categories for security levels over data and permissibility of public disclosure. This could work to avoid situations such as the census - where a person's name, address, age, etc, were all printed for the public eye.
- **Standardization of Privacy Policies and Access Control**
  Government databases should all be designed upon interoperable standards so that the databases can "talk" to each other. The ability to collate databases strengthens the potential for information use and reuse by different stakeholders. Furthermore, the interoperability of systems helps to avoid the creation of silos that hold multiple copies of the same data. To protect the privacy in interoperable systems - restricted and authorized access within departments and between departments is the key. The Department of Information Technology has recently published a "Government Interoperability Framework" titled "Interoperability Framework for eGovernance" This policy document is the appropriate place to articulate interoperable privacy policies that could be adopted across eGovernance projects.
- **Record of breach notification**:
  If data breach occurs in government database, the breach should be recorded and the appropriate individuals notified.
- **Anonymization/obfuscation and deletion policies**
  Once the purpose for which the data has been collected has been served it must be anonymized/obfuscated or deleted as appropriate. All data-sets cannot be deleted as bulk aggregate data is very useful to those interested in trend analysis. Anonymizing/obfuscating the personal details of a data set ensures that privacy is

protected during such trend analysis.

- **Accountability for accuracy of data**
  Frequently data that is collected and entered into government databases is not accurate, because the departments are not collecting the data themselves. Thus, they feel no responsibility for its accuracy. If a mechanism is built into each database for identification of each data source this brings accountability for data accuracy.
- **Appropriate uses of government databases**
  Businesses should not feel automatically entitled to aggregate and consolidate public information from government databases because it is technically possible to do so. Their uses of government database must be guided by policies that define "appropriate usage."
- **Access, updation and control of personal information**
  Citizens must be able to access and update their information. Furthermore, they should be able to define to a certain extent access control to their information - which would automatically make them eligible or ineligible for various government services.

---

1. These include passport, PAN card, ration/ PDS photo card, voter id, driving license, government photo id cards, NREGS job card, photo id issued by a recognized educational institution, arms license, photo bank ATM card, photo credit card, pensioner photo card, freedom fighter photo card, kissan photo passbook, CGHS / ECHS photo card, address card having name and photo issued by department of posts and certificate of identify having photo issued by group a gazetted officer on letterhead, disability ID Card/handicapped medical certificate issued by the respective State/UT. See http://bit.ly/OpsNLA
2. The Passport Act 1967: (Rules 1980), http://bit.ly/11zJNs
3. The Passports Act, 1967, s. 2(c).
4. The Passports Act, 1967, s. 3(a).
5. The Passports Act, 1967, s.10(3)(b).
6. The Passports Act, 1967, s. 10(5).
7. The Passports Act, 1967, s. 11 (1).
8. The Passports Act, 1967, *s.* 12(1)(e).
9. The Passports Act, 1967, s. 1a(b).
10. The Passports Act, 1967, s. 13(1).
11. The Passports Act, 1967, s. 14.
12. The Representation of Peoples Act, 1950, http://bit.ly/RKkTYq
13. See Indian Elections “About Election Commission of India”, http://bit.ly/QlfoCo (last accessed on June 11, 2012).
14. The Representation of Peoples Act, s. 146. These powers include: summoning and enforcing attendance of any person, requiring the production and discovery of any document, requisitioning any public record, issuing commissions for the examination of witnesses or documents.
15. Registration of Elector Rules, 1960, Rule 9 (1961), http://bit.ly/TX1UvB (last accessed on October 30, 2011).
16. Registration of Elector Rules, 1960, Rule 22.

17. Registration of Elector Rules, 1960, Rule 33. Copies of the rolls, including photo rolls, requisitioned by citizens under the Right to Information Act may be provided only if they do not deal with specific third-party individuals. i.e., it is possible to requisition, for instance page 45 of the electoral rolls but it is not possible to specifically requisition the portion of the rolls on which a specific name appears. Hand Book for Electoral Registration Officers Election Commission of India 2008, 56 (2008), http://bit.ly/QlfxG7(last visited on October 30, 2011).
18. Rule 33 of the Registration of Elector Rules, 1960.
19. The Representation of Peoples Act, s. 128.
20. The Representation of Peoples Act, s. 129.
21. The Representation of Peoples Act, s. 136.
22. The Representation of Peoples Act, s. 125A.
23. Indian Penal Code, s. 205.
24. Information Technology Act s. 66 C&D.
25. Section 139A of the Income Tax Act lays down: who can apply for PAN, who will allot PAN, transactions where PAN is required. Rule 114 lays out the process for applying for PAN, Rule 114B lists the documents required, rule 114 C lists exceptions to PAN.
26. Indian Income Tax Act, s. 136.
27. Indian Income Tax Act, s. 131. These include the power to call for information, power of survey, power to collect information , search and seizure
28. What is PAN? http://bit.ly/JbDPQM (last accessed on October 24, 2011).
29. Indian Income Tax Act, s. 139A (5).
30. Indian Income Tax Act, s.133.
31. Indian Income Tax Act, s. 133B.
32. Indian Income Tax Act, s.139A(5)(d).
33. Indian Income Tax Act, s.131 (3).
34. Indian Income Tax Act, s. 138.
35. Income Tax Act, 1961, s. 287.
36. The Census Act, 1948, s. 7(C).
37. The Census Act, 1948, s. 7 (D).
38. The Census Act, 1948, s.15.
39. Census Rules, 1990, Rule 7.
40. The Census Act, 1948, s. 11(1)(b).
41. The Census Act, 1948, s. 11(1)(c).
42. The Census Act, 1948, s.11(1)(f).
43. Census Rules, 1990, Rule 5(4)(a)(iii).
44. Census Rules, 1990, Rule 5(5)(e).
45. Census Rules, 1990, Rule 5(7)(b).
46. Census Rules, 1990, Rule 11(1)(b).
47. Census Rules, 1990, Rule 5(6)(b).
48. Census Rules, 1990, Rule 5 (7)(f).
49. Census Rules, 1990, Rule 9.
50. Census Rules, 1990, Rule 10.
51. Census Act 1948, s. 17, Census Rules 1990, Rule 5(2)(e).
52. Census Rules, 1990, Rule 11.
53. Citizenship Act 1955, http://bit.ly/Q5NIDK, Citizenship Rules 2003, http://bit.ly/TX2byC, Citizenship Rules 2009, http://bit.ly/Q6AQrk
54. Citizenship Act 1955, s. 14A (3).
55. Citizenship (Registration of Citizens and Issue of National Identity Cards) Rules, 2003, Rule 3 (3).
56. Citizenship Rules, 2009, Rule 21.
57. The Citizenship Act 1955, s. 14A.
58. Citizenship Rules 2009, Rules 4(1) and 9.
59. Citizenship Rules 2009, Rule 6(3).
60. Citizenship Rules 2009, Rule 10(3).
61. Citizenship Rules 2009, Rule 8.
62. Citizenship Rules 2009, Rule 4(6)(a).
63. Citizenship Rules 2009, Rule 4(6)(b).

64. Citizenship Rules 2009, Rule 16(5).
65. Indian Citizenship Act, 1955, s. 10.
66. Citizenship (Registration of Citizens and Issue of National Identity Cards) Rules, 2003, Rule 10(3).
67. Indian Citizenship Act, 1955, s. 10(2)(a).
68. Indian Citizenship Act, 1955, s. 17.
69. Indian Citizenship Act, 1955, s. 18.
70. Indian Citizenship Act, 1955, s. 14(1).
71. Citizenship (Registration of Citizens and Issue of National Identity Cards) Rules, 2003, Rule 4(4).
72. Citizenship (Registration of Citizens and Issue of National Identity Cards) Rules, 2003, Rule 4(5)(a).
73. Citizenship (Registration of Citizens and Issue of National Identity Cards) Rules, 2003, Rule 7(a).
74. Citizenship (Registration of Citizens and Issue of National Identity Cards) Rules, 2003, Rule 10.
75. Citizenship (Registration of Citizens and Issue of National Identity Cards) Rules, 2003, Rule 3.
76. Citizenship (Registration of Citizens and Issue of National Identity Cards) Rules, 2003, Rule 12.
77. Registration of Births and Deaths Act, 1969, http://bit.ly/NLP7PA
78. Registration of Births and Deaths Act, 1969, ss. 3,4,6,7.
79. Registration of Births and Deaths Act, 1969, s. 23.
80. Registration of Births and Deaths Act, 1969, s. 17.
81. Registration of Births and Deaths Act, 1969, s. 12.
82. Registration of Births and Deaths Act, 1969, s. 15.
83. Registration of Births and Deaths Act, 1969, s.19.
84. Registration of Births and Deaths Act, 1969, s. 18.
85. Registration of Births and Deaths Act, 1969, s. 19(2).
86. Registration of Births and Deaths Act, 1969, s. 21.
87. Registration of Births and Deaths Act, 1969, s. 30.
88. Information Technology (Electronic Service Delivery) Rules, http://bit.ly/Q5OsZr
89. Information Technology (Electronic Service Delivery) Rules, 2011, Rule 3(3).
90. Information Technology (Electronic Service Delivery) Rules, 2011, Rule 5(1)(2).
91. Information Technology (Electronic Service Delivery) Rules, 2011, Rule 7.
92. Information Technology (Electronic Service Delivery) Rules, 2011, Rule 8.
93. Information Technology (Electronic Service Delivery) Rules, 2011, Rule 5 (4).
94. Information Technology (Electronic Service Delivery) Rules, 2011, Rule 6.
95. Information Technology (Electronic Service Delivery) Rules, 2011, Rule 8(4).
96. Unique Identification Bill 2010, http://bit.ly/R7gQKB
97. Unique Identification Bill, 2010, s. 23(2)(k).
98. Unique Identification Bill, 2010, s. 23(2)(m).
99. Unique Identification Bill, 2010, s. 30.
100. Unique Identification Bill, 2010, s. 23(s).
101. Unique Identification Bill, 2010, s. 30(3).
102. Unique Identification Bill, 2010, s. 33.
103. Unique Identification Bill, 2010, s. 23(2)(l).
104. Unique Identification Bill, 2010, s. 31.
105. Unique Identification Bill, 2010, s. 32.
106. Unique Identification Bill, 2010, ss. 34-40.
107. Unique Identification Bill, 2010, s. 44.
108. Unique Identification Bill, 2010, s. 7.
109. Unique Identification Bill, 2010, s.23(2)(c).
110. Unique Identification Bill, 2010, s. 23(2)(b).
111. Unique Identification Bill, 2010, s. 23(2)(e).
112. Unique Identification Bill, 2010, s. 23(2)(g).
113. Unique Identification Bill, 2010, s. 23(2)(h).
114. Unique Identification Bill, 2010, s.3.
115. Unique Identification Bill, 2010, s. 9.
116. Unique Identification Bill, 2010, s.23(a).
117. Unique Identification Bill, 2010, s. 8.
118. DNA Profiling Bill 2007, http://bit.ly/K4Dooy
119. Center for DNA Fingerprinting and Diagnostics Homepage, http://bit.ly/360clL (last accessed on June 11, 2012).

120. DNA Profiling Bill 2007, s. 1 (xv) –(xvi).
121. DNA Profiling Bill 2007, s. 13 (1) (xv) –(xvi).
122. DNA Profiling Bill 2007, s. 19.
123. DNA Profiling Bill 2007, s. 41(i) (ii).
124. DNA Profiling Bill 2007, ss.45 and 46.
125. DNA Profiling Bill 2007, s. 49 (1).
126. DNA Profiling Bill 2007, s.13(x).
127 . DNA Profiling Bill 2007, s. 22.
128. DNA Profiling Bill 2007, s. (4),(5).
129 DNA Profiling Bill 2007, s.35 (1).
130. DNA Profiling Bill 2012, s. 35.
131. DNA Profiling Bill 2012, s. 32.
132. DNA Profiling Bill 2012, ss. 39 and 40.
133 DNA Profiling Bill 2012, s. 37.
134. "The UK Police National DNA Database," *GeneWatch*, http://bit.ly/Q4BWWb (last accessed on May 15, 2011).
135. "GeneWatch PR: Statement on One Show DNA case (12th January 2011)", *GeneWatch*, http://bit.ly/Q09vLq (last accessed on May 15, 2011).
136. Mr. Sarella Vara Prasada vs. Ministry of External Affairs, CIC, 2011, http://bit.ly/TX2s4v
137. Mr. G. Gururaja Rao vs. Ministry of External Affairs, CIC, 2012, http://bit.ly/RkpY9g
138. Shri Durgesh Vijayvargiya vs Ministry of External Affairs, CIC, 2012, http://bit.ly/OSuxbn
139. P.C. Wadhwa vs Central Information Commission, Punjab & Haryana High Court, 2009, http://bit.ly/TlMPGi
140. Ms. K Sharada vs Ministry of External Affairs, CIC, 2009, http://bit.ly/Q6DwoX
141. "What is a Ration Card and Why is it Needed", *india.gov.in*, http://bit.ly/aFMgYE (last accessed in December 2011).
142. Prodyut Bora, "Identity Crisis: In Search of a Permanent Citizen Identification Scheme", *Times of India*, March 26, 2005", http://bit.ly/OWVlZM (last accessed in December 2011).
143. R. Ramakumar, "What the UID Conceals", *The Hindu*, October 21, 2010, http://bit.ly/bXC5C6 (last accessed in December 2011).
144. "Centre Expands Smart Card PDS across India", *Governance Knowledge Centre*, http://bit.ly/OSvi44 (last accessed in December 2011); "Govt planning multi-use smart ID cards by 2013", *Economic Times*, October 2, 2011 http://bit.ly/n0WI2p (last accessed in December 2011).
145. "Finmin overhauls I-T intelligence to counter tax evasion", *Economic Times*, January 24, 2010, http://bit.ly/OR43IF. According to the article the Central Information Branch is the nodal office in the department to gather all documents pertaining to transactions in relation to which Permanent Account Number (PAN) or General Index Register Number are given during sale and purchase of property and monetary deposits. "*The re-structuring of the Central Information Branch will ensure current, constant and consolidated reporting and delivery of information on transactions, including high value financial ones* which are around Rs 10 lakhs or more," sources said.
146. Deepsikha Sikarwar, "IBA and CBDT join hands to fight black money", *Economic Times*, August 27, 2011, http://bit.ly/TlNAz9 (last accessed on October 24, 2011).
147. Vrishti Beniwal, "Black money info sources to be merged", *Business Standard*, May 4, 2011, http://bit.ly/ldRvge. "Currently, most high-value transactions are reported to the Income-tax department through two channels — Annual Information Return (AIR) and Central Information Branch (CIB).CIB collects information relating to specified transactions for which Permanent Account Number (PAN) is mandatory, such as bank deposits above Rs. 50,000, property deals above Rs. 5 lakh, sale or purchase of a vehicle, opening a bank account, etc. AIR, on the other hand, is furnished by banks, financial institutions, trustees of mutual funds, companies issuing bonds or debentures.
148. Sikarwar, *supra* note.
149. Registration of Elector Rules, 1960, *supra* note at Rule 28.
150. Ashish Chakraborty, "Retention of Old Epic Numbers for New/Duplicate EPICs and Maintenance and Upkeep of Photo-Roll Image Database", 2008, http://bit.ly/UroAWL (last visited on October 30, 2011).
151. *Id.* at para 5.

152. "Coastal villagers of Gujarat to get unique identity card next year", *The Times of India*, June 7, 2009, http://bit.ly/OaCptF (last accessed in December 2011).
153. "The National Identification Authority of India Bill, 2010, *Ministry of Planning*, http://bit.ly/R7gQKB (last accessed in December 2011).
154. Name, father's name, mother's name, spouse name, marital status, nationality as declared, education, occupation, place of birth, present address, duration of address, and permanent address.
155. Fischer Hubner, Simone, "The Future of Identity in the Information Society", *IFIP*, 2008.
156. "Saaransh: A compendium of Mission Mode Projects under NeGP"*, Department of Electronics and Information Technology, Govt. of India,* http://bit.ly/OSw8hd
157. Dr. Rajendra Kumar, "National Population Register"*, Department of Electronics & Information Technology*, http://bit.ly/R7k94F
158. "Your voter ID card may have Aadhaar soon"*, DNA*, May 14, 2012, http://bit.ly/OYaPyo (last accessed on June 7, 2012).
159. "Kerala to be first fully digital state", *The Hindu*, June 5, 2012, http://bit.ly/Kt0j1w (last accessed on June 8, 2012).
160. Devika Banerji, "Home Ministry plans to link its crime records with UIDAI"*, Economic Times*, May 22, 2012, http://bit.ly/NclyFk (last accessed on May 22, 2012).
161. Seema Sindhu, "Home Ministry refuses to use UID data for National I-cards", *The Pioneer*, May 13, 2012, http://bit.ly/K7Hw4P (last accessed on June 8, 2012).
162. Roy, Aruna. "Bring CBI, UID under RTI ambit, says Aruna Roy, *The Times of India*, July 9, 2012, http://bit.ly/PmjV5x. (last accessed September 12th 2012)
163. "DNA profiling of Army personnel to begin soon", *The Times of India*, January 2, 2011, http://bit.ly/Q0b8J4 (last accessed in March 2011).
164. Subhash Chandra Agarwal, "Justice S. Rabindra Bhatt orders DNA test for ND Tiwari", *Merinews*, December 24, 2010, http://bit.ly/fs8OJR (last accessed in June 2011).
165. Shahkar Abidi, "Nehru Nagar first region in country to have DNA profiling database", *DNA*, December 6, 2010, http://bit.ly/fmxR82 (last accessed in December 2011).
166. Adhikary, Jyotirmoy, "DNA Technology in Administration of Justice", p.263, *LexisNexis*, 2007.
167. CDFD. "DNA Fingerprinting", available at http://bit.ly/TX3NrT
168. Ibid. CDFD Annual Report (April 2009 to March 2010), available at http://bit.ly/Q5Ykm1
169 . DLI DNA Research & Forensic Center, available at http://bit.ly/RKtGtj
170. Truth Labs India. http://bit.ly/Qlkgrd
171. Roopak Goswami, "NE to get hi-tech forensic institute", *The Telegraph*, July 7, 2011, http://bit.ly/nW3YIa (last accessed in December 2011); Nikhil S. Dixit, "Mumbai gets it's very first state of the art forensic lab" DNA, November 26, 2006, http://bit.ly/Tb8B5 (last accessed in December 2011); "India may soon have DNA database to crack crime", *The Times of India*, September 15, 2010, http://bit.ly/hAVHqO (last accessed in December 2011).
172. "Most young employees ignore IT policies: Survey", *The Times of India*, January 4, 2012, http://bit.ly/Om8udL(last visited on January 27, 2012).
173. Interview with Basant Shroff: "India suffers from both, too much identification and, too little privacy", *The Financial Express*, September 14, 2012, http://bit.ly/Q5ZCO0 (last visited on January 27, 2012).
174. "Neeraj Chauhan, DU law student charged with cyber stalking", *The Times of India*, July 20, 2011, http://bit.ly/TX41iJ (last visited on January 27, 2012).
175. V Narayan, "Terror SMS from your cell phone number? Possible", *The Times of India*, March 21, 2010, http://bit.ly/NcmWrz (last visited on January 27, 2012).
176. "Dot-conned BJP says Cong stole e-identity", *The Times of India*, Oct, 4, 2010, http://bit.ly/OSBzNh (last visited on Jan. 27, 2012). See the BJP website at http://www.bjp.org/
177. "Guidelines for Technical and Financial Support for Establishment of State Data Centre", *Department of Electronics & Information Technology*, http://bit.ly/NQTCCu
178. "Guidelines for Technical and Financial Support for Establishment of State Data Centre", s. 12.1., *Department of Electronics & Information Technology*.
179. "Guidelines for Technical and Financial Support for Establishment of State Data Centre", ss. 13.1 and 14.1, *Department of Electronics & Information Technology*.
180. "Guidelines for Technical and Financial Support for Establishment of State Data Center",

Department of Electronics & Information Technology, http://bit.ly/NQTCCu
181. Power Point presentation: CSC Seminar Presentations (2011). CSC Building Foundation for Rural Entrepreneurship. (2011).
182. See http://bit.ly/R7k94F
183. See http://bit.ly/aXDF4k
184 . See http://bit.ly/aXDF4k
185. Prashant Iyengar, “India Privacy Country Report”, 2011, *Centre for Internet & Society*.
186. “National Data Sharing and Accessibility Policy”, *Government of India*, 2012, http://bit.ly/TX4cuo
187 . See http://bit.ly/eEfJw3
188. See http://bit.ly/UrrMlj
189. Mohanty, *supra* note.
190. Ibid. Prashant Iyengar, “India Country Report”.
191. “Kerala to be first fully digital State”, *The Hindu*, June 5, 2012, http://bit.ly/Kt0j1w (last accessed on June 8, 2012).
192. “Government to strengthen e-governance initiatives”, *The Times of India*, June 7, 2012, http://bit.ly/OWZpJy (last accessed on June 8, 2012).
193. “Speech by Honorable Prime Minister Shri Manmohan Singh at the inauguration ceremony of Indian Institute of Corporate Affairs Campus (13th April 2012 at IMT Manesar)”, *Ministry of Corporate Affairs*, http://bit.ly/50Cri (last accessed on June 6, 2012).
194. Pankaj Doval, “TCS, Infosys, Wipro vie for e-governance overhaul pie”, *The Times of India*, June 4, 2012, http://bit.ly/M2d9OA (last accessed on June 8, 2012).
195. “Report of the Technology Advisory Group for Unique Projects” (TAGUP), *Ministry of Finance*, http://bit.ly/fItwhc (last accessed on January 31, 2012).
196. TAGUP Report, s. 10.2.
197. TAGUP Report, s. 10.2.1.
198. TAGUP Report, s. 10.2.2.
199. TAGUP Report, s. 10.2.3.
200. “Digitization of Land Records: Bhoomi Project”, Government of Karnataka, http://bit.ly/93WaDC
201. Caryn Mladen, recommendations drawn and adopted from “A Report of Research on Privacy for Electronic Government”, Privacy in Canada, available at http://bit.ly/TlFok2